UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2018 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW GATREL, aka "Fluffy," and JUAN MARTINEZ aka "Severon," Defendants.	CR No. 19-CR00036-JAK I N D I C T M E N T [18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud; 18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)(i), (c)(4)(A)(i)(VI): Unauthorized Impairment of a Protected Computer; 18 U.S.C. § 2: Aiding and Abetting and Causing an Act to be Done]

The Grand Jury charges:

COUNT ONE

[18 U.S.C. § 371]

A. OBJECT OF THE CONSPIRACY

Beginning on an unknown date but prior to October 10, 2014, and continuing to on or about November 19, 2018, in Los Angeles County, within the Central District of California, and elsewhere, defendants MATTHEW GATREL, also known as ("aka") "Fluffy" ("GATREL"), and JUAN MARTINEZ, aka "Severon" ("MARTINEZ"), and others known and unknown to the Grand Jury, knowingly conspired

and agreed with each other to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and specifically to cause such damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI).

B. MEANS BY WHICH THE OBJECT OF THE CONSPIRACY WAS TO BE ACCOMPLISHED

The object of the conspiracy was to be accomplished in substance as follows:

1. Defendant GATREL, using a computer or computers in Illinois, would offer services via the website downthem.org that would allow his subscribers, for a fee, to cause floods of Internet traffic to be directed to victim computers, an online attack technique known as "Distributed Denial of Service" or "DDoS," for the purpose of degrading or disrupting the victim computers' access to the Internet.

2. Defendant GATREL would construct these DDoS attacks to use a practice known as "amplification," meaning that brief commands sent to third-party computers and devices would cause much longer strings of data to be sent back in response.

3. Defendant GATREL would regularly investigate and keep updated lists of computers and devices connected to the Internet that could be electronically queried to cause these amplified floods of Internet traffic to be sent to victims, without the permission of the owners of those computers and devices.

//

4. Defendant GATREL would construct the attacks in such a manner as to disguise the true origin of the electronic queries sent to such computers and devices, so that the computers and devices sending the floods of Internet traffic perceived the queries to be coming from the victim computers rather than GATREL or his subscribers, a practice known as "spoofing."

5. Defendant MARTINEZ, using a computer or computers in California, would communicate with and assist GATREL in the operation of the downthem.org services.

6. Defendants GATREL and MARTINEZ, and other unindicted co-conspirators, would maintain and improve the downthem.org website and services, and respond to requests for attacks, subscriptions, or assistance from potential or current customers.

7. Defendant GATREL would also offer a server subscription service via the website ampnode.com that would allow subscribers to obtain use of servers suitable for operating their own DDoS attack services or conducting their own DDoS attacks from infrastructure controlled and managed by the customer.

8. GATREL would work with other persons, including an individual representing a hosting company based in Eastern Europe, to secure the servers that GATREL then resold.

9. Defendant GATREL would generate lists of vulnerable computers and devices and then sell such lists to customers via the ampnode.com site for the purpose of assisting customers with conducting large-scale DDoS attacks.

C. OVERT ACTS

In furtherance of the conspiracy and to accomplish its object, defendants GATREL and MARTINEZ, and others, committed

various overt acts within the Central District of California, and elsewhere, including but not limited to the following:

Overt Act No. 1: On or about August 19, 2015, defendant GATREL sent a message to a customer via the downthem.org website discussing the various methods available to cause floods of data to be sent to victim computers, including protocols that would rely on "spoofing."

Overt Act No. 2: On or about September 7, 2015, defendant GATREL sent a message to a customer via the downthem.org website stating that any of his available methods would work to shut down a home Internet connection, and suggesting particular protocols that that would rely on "spoofing."

Overt Act No. 3: On or about October 4, 2015, defendant GATREL sent a message to a customer via the downthem.org website providing advice on the best protocol to use to "down xbox live targets," noting that he personally did "15 second chargen hits" to knock players out of online games.

Overt Act No. 4: On or about October 7, 2015, defendant GATREL posted a message on the downthem.org website stating that he had updated the power of the site and thanking every customer, stating that it was only by way of his customers that the site was possible. Defendant GATREL added that customers who referred their friends to the site would get bonus time added to their accounts for free.

Overt Act No. 5: On or about November 19, 2015, in response to a customer request to help the customer "get [] back" at an online game service by "taking down" their server, defendant GATREL sent a message via the downthem.org website to

the customer saying that he would not do so for free, but would conduct tests to see if the server was "downable."

Overt Act No. 6: On or about November 22, 2015, in response to a customer request for help with taking down a server, defendant GATREL sent a message via the downthem.org website to the customer saying that he would attempt to find vulnerable ports for the customer, noting that the target was a server hosted by a large server-hosting company but it was still possible to make it "go down."

Overt Act No. 7: On or about November 22, 2015, in response to a customer seeking "some revenge" on someone who had sent the customer DDoS attacks, namely, by severely interrupting the victim's server's connection or taking down the victim's server for a while, defendant GATREL sent a message via the downthem.org website to the customer recommending a particular attack protocol.

Overt Act No. 8: From on or about November 25, 2015 through on or about November 26, 2015, in response to a customer's expressed inability to take down a server using the downthem.org service, defendant GATREL sent a series of messages via the downthem.org website to the customer offering his assistance and suggesting attack methods; in response to the customer's inquiry about using a botnet instead, defendant GATREL said that the customer should try to attack with the methods defendant GATREL had on his site, adding that the more customers he had, the more power would be available via the site.

Overt Act No. 9: On or about January 18, 2017, in response to a customer request to "destroy" a server hosted by a

large server hosting company and offering to advertise the downthem.org site via video on the website YouTube, defendant GATREL advised the customer that the customer would need a "corporate" level subscription to "destroy" such a server, and offered discounts if the customer advertised and made a good video.

Overt Act No. 10: On or about July 6, 2017, defendant GATREL sent a message via the downthem.org website to a customer saying that defendant GATREL updated the downthem.org site almost daily, and he had numerous methods for amplification - that is, numerous methods in which to conduct DDoS attacks against victim computers and devices, including methods that used "spoofing" and other protocols for traffic amplification.

Overt Act No. 11: On or about July 7, 2017, in response to the customer's inquiry about attacking the "official servers" for certain gaming platforms, defendant GATREL sent a message via the downthem.org website to the customer saying that it was difficult to "knock off" such professionally hosted servers, but some of his customers had had success with some of his available attack methods, and that the methods "worked great" once you identified an open port on the victim server.

Overt Act No. 12: On or about April 22, 2017, defendant GATREL posted an update on the downthem.org website saying that the site was "still going strong" so that everyone would know "everything was still running smooth" and that he hoped everyone continued to enjoy the great service every day.

Overt Act No. 13: On or about July 15, 2017, defendant GATREL told a customer of ampnode.com in an email that defendant

GATREL had just updated his list of vulnerable servers that could be enlisted to send attacks to victim computers using "spoofing" and other amplification methods.

Overt Act No. 14: On or about August 6, 2017, defendant GATREL posted the following message on the downthem.org site: "I would first like to thank every new and every recurring customer. I appreciate your business and your loyalties and it is only by way of you all knowing which service has the absolute strongest and honest power to effect EVERY SINGLE ONE OF YOUR TARGETS with ease that make this website possible. We are also celebrating running for more than 8 years which no other site has even come close to accomplishing!!!!! Our power is again over 100Gbps easily. We're down'ing NFO, OVH, and even some reported down'ing Vox. Our new methods are very powerful and custom so other sites can't match! If you refer your friends you WILL get BONUS time added to your account for FREE. This site is not like others; the more customers we have the power I add for everyone to use and enjoy."

Overt Act No. 15: Between on or about January 16, 2018, and January 18, 2018, in response to a customer request to take down a target while running four to six attacks at the same time, defendant GATREL sent a series of messages to the customer via the downthem.org website, saying that he would conduct some tests and see if an associate could do more with a botnet as well; defendant GATREL proceeded to explain to the customer how his service worked, by sending a command through the source server to "hundreds, sometimes hundreds of thousands of relay servers and those servers are told to send little data packets to a victim."

Overt Act No. 16: On or about April 26, 2018, in response to a customer request about how downthem.org compared to other services, defendant GATREL sent a message via the downthem.org website to the customer saying that what set his site apart was that it had been running since 2007 and more customers using the site translated to more servers available for attacks, and thus "more total output."

Overt Act No. 17: Between on or about May 28, 2018 and on or about May 30, 2018, in response to a customer request for a custom product and "spoofing servers," defendant GATREL sent a series of messages to the customer via the downthem.org website clarifying that the customer was seeking to set up a product via defendant GATREL's ampnode.com service, and providing advice on what server would best suit the customer's needs, including particular attack method availability. Defendant GATREL added that his technician would be able to help in setting up the requested server, and that defendant GATREL updated his lists of vulnerable computers and devices to use for attacks at least once a week.

Overt Act No. 18: Between on or about September 8, 2018 and on or about September 11, 2018, defendant MARTINEZ sent a series of messages via the downthem.org site to defendant GATREL about redesigning and improving the downthem.org site and offering to work with GATREL on the site and associated services.

Overt Act No. 19: Between on or about September 17, 2018 and on or about September 20, 2018, in response to a customer request for help in taking down a game server, defendant GATREL sent a series of messages to the customer via the downthem.org

website suggesting various methodologies, and saying that he would present the information from the customer to defendant MARTINEZ to work on an effective exploit.

Overt Act No. 20: Between on or about September 20, 2018 and on or about October 11, 2018 defendant MARTINEZ sent a series of messages to the same customer via the downthem.org website to continue discussing how to attack the specific game the customer was targeting.

Overt Act No. 21: On or about October 13, 2018, in response to a customer's request to shut down two websites, defendant MARTINEZ sent the customer a message via the downthem.org website saying that he and defendant GATREL had been discussing the customer's request, but they would need to increase the attack power to 900 Gigabits, which would cost $1000 per week; defendant MARTINEZ added that he guaranteed that the sites would be offline as long as the customer rented his and GATREL's services.

Overt Act No. 22: On or about October 16, 2018, defendant MARTINEZ sent a customer a message via the downthem.org website regarding the best method for "spoofing," and saying that it was hard to know how much power would be needed to shut down the server the customer wished to target until they tried, but if 300 Gigabits did not slow it down they would add "more and more servers till [it] collapses."

Overt Act No. 23: On or about October 17, 2018, defendant GATREL sent the same customer a message, stating that defendant GATREL would allow the customer to run four DDoS attacks concurrently, and that defendant MARTINEZ would have a better

idea of how to take the down the service the customer was targeting.

Overt Act No. 24: On or about October 17, 2018, defendant MARTINEZ sent the same customer a message, stating that he and defendant GATREL had been adding more "hitting power" to their service, and describing how to effectively attack the customer's target.

Overt Act No. 25: On or about October 20, 2018, defendant GATREL sent the same customer another message, stating that as more customers came to the downthem.org site, more power would get added, but they were already doing well over 600 Gigabits per second of power - "more power than any other website like this" - and adding that even the best-protected servers around were impacted by his service.

COUNT TWO

[18 U.S.C. § 1349]

A. OBJECT OF THE CONSPIRACY

Beginning on an unknown date but prior to October 10, 2014, and continuing to on or about November 19, 2018, in Los Angeles County, within the Central District of California, and elsewhere, defendants MATTHEW GATREL, also known as ("aka") "Fluffy" ("GATREL"), and JUAN MARTINEZ, aka "Severon" ("MARTINEZ"), and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

B. MEANS BY WHICH THE OBJECT OF THE CONSPIRACY WAS TO BE ACCOMPLISHED

The Grand Jury hereby repeats and realleges the Means by Which the Object of the Conspiracy Was to be Accomplished set forth in Section B of Count One of this Indictment as if fully set forth herein.

C. OVERT ACTS

The Grand Jury hereby repeats and realleges the Overt Acts set forth in Section C of Count One of this Indictment as if fully set forth herein.

COUNT THREE

[18 U.S.C. §§ 1030(a)(5)(A), (b), (c)(4)(B)(i), (c)(4)(A)(i)(VI); 2(a), 2(b)]

Beginning on an unknown date but prior to October 10, 2014, and continuing to on or about November 19, 2018, in Los Angeles County, within the Central District of California, and elsewhere, defendants MATTHEW GATREL, also known as ("aka") "Fluffy," and JUAN MARTINEZ, aka "Severon," knowingly caused and knowingly and intentionally aided and abetted the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage and attempted to cause damage by impairing the integrity and availability of data, programs, systems, and information on protected computers, as that term is defined in Title 18 United States Code, Section 1030(e)(2)(B), thereby causing and attempting to cause damage affecting ten or more protected computers during a one-year period beginning on or about November 20, 2017.

FORFEITURE ALLEGATION ONE

[18 U.S.C. §§ 982 and 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1030, and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offenses set forth in any of Counts One and Three of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

a. All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

b. Any property used or intended to be used to commit the offense; and

c. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i), the convicted defendant shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been

transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offense set forth in Count Two of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

a. all right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

b. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), the convicted defendant shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or

//

(e) has been commingled with other property that cannot be divided without difficulty.

A TRUE BILL

_____
Foreperson

NICOLA T. HANNA
United States Attorney

PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division

RYAN WHITE
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

CAMERON L. SCHROEDER
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section